

SECURE CONFIGURATION OF A DIGITAL CERTIFICATE FOR A PRINTER OR OTHER NETWORK DEVICE

Abstract of the Disclosure

5 The system, method, and program of this invention provides a secure
configuration of a digital certificate for a printer. The printer has a unique
encryption key stored in it at manufacturing time. This key is also recorded in
a database, securely controlled by a certificate authority, and the key is
associated with the printer by model and serial number. The printer sends a
message requesting a digital certificate to the certificate authority. In the
10 message request, the printer sends the model number and serial number of the
printer in the clear, i.e., not encrypted, which is needed by the certificate
authority to look up the unique encryption key in the database. The message
request also contains an encryption, using the built-in key, of some of the same
information that was sent in the clear. The database needs the information in
15 the clear to get the key. Then, the database uses the key from its database to
decrypt the encrypted part of the message, and compares it to the part of the
message that was sent in the clear. If it matches, then the program operating
with the database knows that the message has not been tampered with and
that the printer is who it says it is. The database machine then creates the
20 digital certificate and encrypts the certificate with the key from its database
corresponding to that printer. The encryption key is a secret key only known

by the printer and the database. The encrypted certificate is sent to the printer and stored in the printer for use in authenticating itself to others.

10004516-110301